



December 18, 1972
NUMBER 5200.28

ASD(C)

Department of Defense Directive

SUBJECT Security Requirements for Automatic Data Processing
(ADP) Systems

- Refs:
- (a) DoD Directive 5100.40, "Responsibilities for the Administration of the Automatic Data Processing Program," May 18, 1970
 - (b) DoD Directive 4105.55, "Selection and Acquisition of Automatic Data Processing Resources," May 19, 1972
 - (c) DoD Directive 5135.1, "Assistant Secretary of Defense (Telecommunications)," January 11, 1972
 - (d) DoD Directive 4630.1, "Programming of Major Telecommunications Requirements," April 24, 1968
 - (e) through (l) see enclosure 1

I. PURPOSE

A. This Directive:

1. Establishes uniform policy for protecting classified data stored, processed, or used in, and classified information communicated, displayed, or disseminated by an Automatic Data Processing (ADP) System, including systems capable of time or resource sharing, having remote access input/output (I/O) terminals, and containing all levels of classified material.
2. Permits the application of access and distribution limitations imposed on classified data and information, in addition to the controls required by the security classification of the material.

3. Specifies conditions and prescribes security requirements under which ADP Systems will be operated when handling classified material and assigns responsibility for the testing, evaluation, and approval of such systems.
4. Provides for the application of administrative, physical, and personnel security measures required to protect ADP equipment, material, and installations (resources) from inadvertent or deliberate compromise, theft, damage, or destruction.
5. Authorizes the publication of (a) a Department of Defense Manual of Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating - Secure Resource Sharing ADP Systems (5200.28-M), and (b) a Department of Defense Computer Security News Letter which will provide periodic information about on-going secure ADP System implementation and testing or other related ADP security matters of DoD-wide interest.

B. Its objectives are to establish that:

1. Security controls for ADP Systems are interrelated with normal internal system controls, such as, input/output controls, program execution controls, operating controls, and internal check procedures.
2. The reliability, integrity, and operation of an ADP System is enhanced by the imposition of many of the controls which satisfy security requirements.
3. The basic ADP System reliability and integrity features must be augmented to assure that systems which process, store, or use classified data and produce classified information will, with reasonable dependability, prevent
 - a. Deliberate or inadvertent access to classified material by unauthorized persons, and
 - b. Unauthorized manipulation of the computer and its associated peripheral devices.

Dec 18, 72

5200.28

II. APPLICATION AND SCOPE

The provisions of this Directive apply to the Office of the Secretary of Defense and to all Department of Defense (DoD) Components (The Military Departments, Defense Agencies, the Organizations of the Joint Chiefs of Staff, and Unified and Specified Commands) which handle (process, store, use, or produce) classified material in ADP Systems; and it covers such systems when operated by contractors and by computer service organizations providing contractual ADP services to DoD Components or their contractors.

III. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

IV. POLICY

The protection of classified material in an ADP System shall be in accordance with that required in DoD Directive 5200.1, and DoD Regulation 5200.1-R, references (e) and (f). Classified material contained in an ADP System shall be safeguarded by the continuous employment of protective features in the system's hardware and software design and configuration; and by other appropriate administrative, physical, personnel, and communication security controls. The potential cost of the ADP System dictates that the security policy, contained herein, be judiciously implemented, carefully managed, regularly reviewed, and continuously monitored to assure the most effective and economical use of the ADP System and related resources of the Department of Defense and, where applicable, of its contractors.

A. Each Department of Defense Component shall:

1. Assure that internal ADP Systems conform to the policy stated herein.
2. Observe closely and use the fundamental computer security policy, concepts, and measures outlined in this Section and Section VI, when designing, procuring, adopting, or operating ADP Systems for the processing, storage, use, and production of classified material.

3. Assure that the diversity and complexity of existing DoD owned ADP Systems and those already designed for future placement which may not presently provide for the complete compliance with the provisions of this Directive contain security measures which provide alternative solutions to the security problems which, in part, are dependent upon the individual characteristics of the ADP System, and its usage.

B. Generally, security of an ADP System is most effective and economical if the system is designed originally to provide it. Each Department of Defense Component undertaking design of an ADP System which is expected to process, store, use, or produce classified material shall:

1. From the beginning of the design process, consider the security policies, concepts, and measures prescribed in this Directive.
2. When evaluating alternative design approaches, consider together the functional system, the ADP equipment, the telecommunications facilities, and the security requirements. Select for implementation the design alternative offering the most economical balance of elements which meet the total system requirements.

C. Recognizing both the validity of the security requirements in this Directive and the difficulty involved in their application to currently installed and already designed ADP Systems, a DoD Component may process, store, or use classified data and produce classified information in an ADP System that is:

1. Operating in a dedicated mode (encl. 2, 7.) full time or for specific periods of time when all users with access to the system have a clearance and need-to-know for all data and information then contained in the system;

DACS IS
DEDICATED AT
TS LEVEL

- a. In such cases the requirements of Section VI. are normally fulfilled by the access, personnel, administrative, physical, and communication security controls established for (1) the Central Computer Facility, (2) the ADP System's interconnecting communication links, (3) all peripheral devices, (4) input/output terminals,

Dec 18, 72
5200.28

and (5) remote terminal areas connected to the system. These controls shall be in conformity with those required for the protection of the highest classification and most stringent access restrictions assigned to the material being handled in the system.

- b. After the User(s) has stored or made proper disposition of all of the classified material and the media used to store the classified material has been secured or erased (declassified), the ADP System may be returned to its original state or to an unclassified and undedicated state, as appropriate.

2. Operating in a controlled environment in a security mode that the Designated Approving Authority (V.C.) or higher authority has determined will achieve and maintain the degree of security that is consistent with the intent of this Directive.
3. Operating in a true multi-level security mode (encl. 2, 10.) using all essential hardware/software security features in the ADP System, in addition to the administrative, physical, personnel, and communication security controls needed to meet the requirements of Section VI. and the overall intent of this Directive. (Techniques and procedures which can be used to secure, test, and evaluate resource sharing ADP Systems are contained in DoD Manual 5200.28-M.)

- a. The head of a DoD Component or his Designated Approving Authority (V.C.) may authorize temporary exceptions to specific security measures which they have determined would impair operation and mission effectiveness, provided he assures that continuous progress is made toward the ultimate full compliance with the Directive at the earliest practicable time. Authority to authorize these temporary exceptions shall not be further delegated. (Also see subsections 1 and 2 above.)

- b. Temporary exceptions to specific security measures for ADP Systems which contain compartmented intelligence or SIOP-ESI, however, shall be subject to the prior approval of the appropriate authority in Sections V.F., G., and H. below. (DIRECTOR, DIA)

- D. When a peripheral device or remote terminal, whether or not
- Approved For Release 2004/02/10 : CIA-RDP79M00096A000100070001-8

personnel of a Component that is not responsible for the overall operation and control of the ADP System, the security measures for the device or terminal and its area shall be prescribed by the authority responsible for the security of the over-all ADP System. Such security measures shall be agreed to and implemented before the user's peripheral device or remote terminal may be connected to the ADP System.

E. When one or more DoD Components' ADP Systems become a part of a larger teleprocessing network (e.g., the Intelligence Data Handling System Communication Network, under the cognizance of DIA or the Worldwide Military Command and Control Systems under the cognizance of the JCS), the approval and the authority to authorize temporary exceptions to security measures for the Components' ADP System in the network shall require the concurrence and approval of both the DoD Component operating the ADP System and the DoD Component having over-all responsibility for the security of the network.

1. As in C. above, the authority responsible for the over-all operation and control of the network shall determine the security requirement for the Systems which are to be connected to the network; and such measures shall be agreed to and implemented before a user's ADP System is connected to the network.
2. This concept, however, does not include ADP Systems which require only communications support from telecommunications networks, such as AUTODIN. In such cases, the DoD Component that controls the ADP System shall determine the security requirements for the classified material handled in the ADP System. The security measures to be agreed to and implemented in such cases shall be limited to those needed to insure the development, interface, and integration of secure, reliable, survivable, and cost-effective transmission and communication lines and links needed to meet the communication requirements of the telecommunications network supporting the ADP System (see F. below).

F. Transmission and communication lines and links which provide secure communications between components of or to an ADP System shall be secured in a manner appropriate for the material designated for transmission through such lines or links under the provisions of DoD Directive C-5200.5, reference (g) and DoD Regulation 5200.1-R, reference (f). Telecommunications

Dec 18, 72
5200.28

facilities supporting ADP Systems shall meet the security criteria used for the Defense Communications System and the criteria for equipment interfacing with such systems.

- G. Measures to control compromising emanations shall be approved under the provisions of DoD Directive S-5200.19, reference (h), by the cognizant authority within the Component operating the ADP System. These measures within industrial ADP Systems, however, shall be applied only at the direction of the contracting activity concerned under provisions of O., below and such requirements shall be included in the contract.
- H. Disconnect procedures, when required to protect classified material contained in the ADP System, shall be used to disconnect remote I/O terminals and peripheral devices from the system by a hardware or software method authorized by the Designated Approving Authority (V. C.).
- I. Procedures and basic safeguards prescribed in DoD Regulation 5200.1-R, reference (f), for the transmission, processing, handling, storage, and disposal of classified information apply to the protection of classified end products produced by the ADP System.
- J. Security measures for ADP Systems which are integral or adjunctive to the control of weapons, communications, or to tactical level data exchange systems, shall be established concurrently with the design and development of the system using fundamental security concepts outlined in this Directive.
- K. When RESTRICTED DATA or FORMERLY RESTRICTED DATA is introduced into an ADP System, appropriate personnel and physical security measures shall be implemented in conformance with DoD Directive 5210.2, reference (i).
- L. Measures to protect compartmented intelligence contained in an ADP System shall also meet the minimum security requirements of DCID No. 1/16, reference (k).
- M. Measures to protect SIOP-ESI, contained in an ADP System, shall also meet minimum security requirements of SM 212-72, reference (l).

- Approved For Release 2004/02/10 : CIA-RDP79M00096A000100070001-8
- N. Material having special controls indicating restricted handling for which systems of compartmentation or handling are;

formally established shall not be introduced into any existing ADP System that has not been dedicated to, or designed and approved for, the handling of compartmented intelligence, SIOP-ESI, or such other information, except or until:

1. The responsible parties within, or between, concerned DoD Components or elements of a DoD Component, have assessed the impact, including costs, of the security measures to be added to the system by reason of the introduction of such material into the ADP System; and
2. The Designated Approving Authority (V. C.) within the DoD Component which operates the ADP System has agreed to the conditions and implements the security measures required for such operations; and
3. The concerned activities have established contingency plans, schedules, priorities, and agreements to assure the most effective operation of the ADP System in support of DoD objectives, have determined those emergency conditions which will affect priorities, and have provided directions under which security measures are waived in favor of operational necessities; and
4. Approval of the ADP System has been obtained in accordance with Subsections V.F., G., and H. **DIA APPROVAL**

- O. Subject to the provisions of Subsections V.F., G., and H., below, TOP SECRET material or material having special controls indicating restrictive handling for which systems of compartmentation and handling are formally established shall not be introduced into a contractor's ADP System except when the system is operating in a dedicated mode and under such other restrictions as shall be determined jointly by the contracting DoD Component and the DSA. Applicable restrictions and instructions shall be included in the contract.
- P. Whenever material requiring special controls (L. and M. above) is withdrawn from the ADP System, or when the required level of protection is reduced for any other legitimate reason, the system shall be operated under the controls appropriate for the material remaining in the system.

Dec 18, 72
5200.28

V. RESPONSIBILITIES

- A. The Assistant Secretary of Defense (Comptroller) (ASD(C)), or his designee for this purpose, in addition to the over-all ADP responsibilities assigned under DoD Directive 5100.40, reference (a), shall:
1. Develop and monitor over-all security policy, standards, and criteria applicable to ADP Systems under this program in accordance with DoD Directive 5200.1 and DoD Regulation 5200.1-R, references (e) and (f).
 2. Publish and maintain in up-to-date form, a Department of Defense Manual 5200.28-M, "Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating - Secure Resource Sharing ADP Systems", and periodically publish a "Department of Defense Computer Security News Letter", providing information on ADP security matters of DoD-wide interest.
 3. Establish a central DoD capability for:
 - a. Assisting and advising DoD Components in ADP System security testing and evaluation;
 - b. Assessing progress of DoD Components toward development and effective installation of secure ADP Systems.
 4. Assure that potential commercial suppliers of ADP resources (DoD Directive 4105.55, reference (b)) are apprised of these and any subsequent security requirements so that security features may be considered by the procurement authority in the acquisition of new ADP Systems or equipment, and commercial ADP research and development may be directed toward improved computer security techniques in the immediate future.
 5. Represent the Department of Defense on Interagency Committees engaged in the development of policy, standards, and criteria for implementing, deactivating, testing, and evaluating secure resource-sharing ADP Systems.

6. Act as Chairman of an ADP System Security Task Force made up of representatives from the intelligence, telecommunications, command and control, and collateral (Army, Navy, Air Force and Defense Agencies) communities that shall review, evaluate, and recommend adoption of policy, standards, criteria, tools, and techniques that shall have application to more than one DoD Component or industry for securing, testing, and evaluating ADP Systems designated to handle classified information.
- B. The Assistant Secretary of Defense (Telecommunications), in accordance with responsibilities assigned under DoD Directive 5135.1, reference (c), shall insure that adequate mechanisms exist for the development and procurement of integrated secure means of telecommunications in support of secure ADP Systems.
- C. The Head of each DoD Component shall: Designate an official(s) as a Designated Approving Authority (e.g., a Senior ADP Policy Official; designated under DoD Directive 5100.40, reference (a), etc.,) to approve ADP Systems for the processing, use, storage, and production of classified material under their jurisdiction. It shall be the responsibility of each Designated Approving Authority to: *Senior ADP Policy Official for DA = ASA (FM)*
AR18-1 { ADP PROGRAM MANAGER FOR DA = DMIS
 1. Assure that such ADP Systems meet and maintain the requirements prescribed for the system, and that the continued approval of the system is contingent upon the results of a recurring review, testing, and favorable evaluation of the security features and cost effectiveness of the system.
 2. Manage, or, assign responsibility to subordinate organizations to manage, the implementation of ADP System security policy and the testing and evaluation of the security features of ADP Systems under their jurisdiction.
 3. Provide for the appointment of a responsible ADP System Security Officer for each ADP System approved for the handling of classified material. *NOT JUST COMPARTMENTED!*
- D. The Secretary of the Navy, in addition to the responsibilities outlined in C., above, through the DoD Computer Institute (DoDCI), shall also provide training for ADP System users, computer specialists, and security specialists who will be engaged in the development, management, and operation of secure ADP Systems.

Dec 18, 72
5200.28

- E. The Director, Defense Supply Agency (DSA), shall also designate one or more officials to approve contractor ADP Systems for the handling of classified material, and when required, certify, on behalf of the Director, DSA, those industrial systems which meet prescribed requirements, to the responsible authority designated in Subsections F., G., and H. below, for approval:
- F. The Director, National Security Agency (NSA), shall:
1. Adopt appropriate security measures consistent with the intent of this Directive for ADP Systems under his control, including those of NSA contractors.
 2. Provide DoD Components, as requested, communications security assistance in support of effective ADP security measures.
- G. The Director, Defense Intelligence Agency (DIA), shall:
1. Approve as required, ADP Systems of DoD Components and their contractors, except for the systems under the cognizance of the NSA which operate in the compartmented mode of operation as defined in DCID No. 1/16, reference (k), to process, store, use, or produce compartmented intelligence.
 2. Advise the Director, Joint Staff, of those ADP Systems which have been accredited under DCID No. 1/16, reference (k) (see G. 1., above) which also handle SIOP-ESI.
- H. The Director, Joint Staff, shall monitor implementation of security policy, approve ADP Systems, and permit temporary exceptions to security measures, as required, for ADP Systems of DoD Components and their contractors which will process, store, use, or produce SIOP-ESI under the provisions of SM 212-72, reference (1).

VI. MINIMUM REQUIREMENTS

A. The objectives of this Directive will be accomplished by ADP System Security Features and Measures that insofar as possible provide:

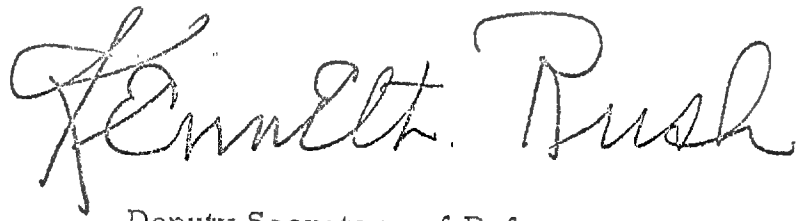
1. Individual Accountability. Each user's identity shall be positively established, and his access to the system, and his activity in the system (including material accessed and actions taken) controlled and open to scrutiny.
2. Environmental Control. The ADP System shall be externally protected to minimize the likelihood of unauthorized access to system entry points, access to classified information in the system, or damage to the system.
3. System Stability. All elements or components of the ADP Systems shall function in a cohesive, identifiable, predictable, and reliable manner so that malfunctions are detected and reported within a known time.
4. Data Integrity. Each file or collection of data in the ADP System shall have an identifiable origin and use. Its accessibility, maintenance, movement, and disposition shall be governed on the basis of security classification and need-to-know.
5. System Reliability. The system shall function so that each user has access to all of the information to which he is entitled, but no more.
6. Communication Links. These links and lines shall be secured in a manner appropriate for the material designated for transmission through such lines or links.
7. Classified Material. Such material handled and produced by the ADP System or stored in or on media for recording classified material shall be safeguarded as appropriate for the classification assigned to the information.

Dec 18, 72
5200.28

- B. The principles in Subsection A., above, shall be implemented by the application of appropriate security measures. Application of such measures shall be the basis for the initial testing and evaluation leading to the approval or disapproval of the ADP System. These security measures are to be upgraded as experience and new techniques are acquired under actual operating conditions or as a result of follow-on testing and evaluation procedures. (Some of the techniques and measures which may be used to secure systems operated in the multi-level Security Mode are contained in DoD Manual 5200.28-M.)

VII. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Two (2) copies of each implementing document shall be forwarded to the Assistant Secretary of Defense (Comptroller) within ninety (90) days. One copy shall be appropriately marked to indicate the implementation of all parts of this Directive.



Deputy Secretary of Defense

Enclosures - 2

1. List of References (Continued)
2. Definitions

5200.28(Encl 1)
Dec 18, 72

- (e) DoD Directive 5200.1, "DoD Information Security Program," June 1, 1972
- (f) DoD Regulation 5200.1 (R), "DoD Information Security Program," June 1, 1972
- (g) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," April 13, 1971
- (h) DoD Directive S-5200.19, "Control of Compromising Emanations (U)," February 10, 1968
- (i) DoD Directive 5210.2, "Access to and Dissemination of Restricted Data," October 18, 1968
- (j) DoD Directive 5220.22, "Department of Defense Industrial Security Program," July 30, 1965
- (k) DCID No. 1/16, "Security of Compartmented Computer Operations," January 7, 1971*
- (l) SM 212-72, "Policy for Safeguarding the Single Integrated Operational Plan," (U), May 12, 1972*

* Copies available on a need-to-know basis from Director, Defense Intelligence Agency or the Director, Joint Staff, OJCS, as appropriate.

5200.28(Encl 2)
Dec 18, 72

DEFINITIONS

1. Access

The ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in an ADP System.

2. Automatic Data Processing (ADP) System

An assembly of computer equipment, facilities, personnel, software, and procedures configured for the purpose of classifying, sorting, calculating, computing, summarizing, storing, and retrieving data and information with a minimum of human intervention. ADP Systems as defined for purposes of this directive are the totality of Automatic Data Processing Equipment (ADPE) and include:

- a. General and Special purpose computers (e.g., digital, analog, or hybrid computer equipment);
- b. Commercially available components, those produced as a result of Research and Development, and the equivalent systems created from them, regardless of size, capacity, or price, which are utilized in the creation, collection, storage, processing, communication, display, and dissemination of classified information;
- c. Auxiliary or accessorial equipment, such as, data communications terminals, source data automation recording equipment (e.g., optical character recognition equipment, paper tape typewriters, magnetic tape cartridge typewriters, and other data acquisition devices), data output equipment (e.g., digital plotters and computer output microfilmers), etc., to be used in support of digital, analog, or hybrid computer equipment, either cable-connected, wire-connected, or self-standing;
- d. Electrical accounting machines (EAM) used in conjunction with or independently of digital, analog, or hybrid computers; and

5200.28 (Encl 2)
Dec 18, 72

- e. Computer equipment which supports or is integral to a weapons system.

3. ADP System Security

Includes all hardware/software functions, characteristics, and features; operation procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities; and, the management constraints, physical structures, and devices; personnel and communications controls needed to provide an acceptable level of protection for classified material to be contained in the computer system.

4. Central Computer Facility

One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area. This does not include remote computer facilities, peripheral devices, or terminals which are located outside the single controlled area even though they are connected to the central computer facility by approved communication links.

5. Compartmented Intelligence includes only that intelligence material having special controls indicating restrictive handling for which systems of compartmentation or handling are formally established.

6. Contained

"Contained" refers to a state of being within limits, as within system bounds, regardless of purpose or functions, and includes any state of storage, use, or processing.

7. Dedicated Mode

An ADP System is operating in a dedicated mode when the central computer facility and all of its connected peripheral devices and remote terminals are exclusively used and controlled by specific users or groups of users for the processing of a particular type(s) and category(ies) of classified material.

8. Intelligence

Intelligence is the product resulting from the collection, evaluation, and interpretation of all information

5200.28 (Encl 2)
Dec 18, 72

concerning one or more aspects of foreign countries or areas, which is immediately or potentially significant to the development and execution of plans, policies, and operations.

9. Material

"Material" refers to data processed, stored, or used in, and information generated by, an ADP System regardless of form or medium, e.g., programs, reports, data sets or files, records, and data elements.

10. Multi-Level Security Mode

An operation under an operating system (supervisor or executive program) which provides a capability permitting various levels and categories or compartments of material to be concurrently stored and processed in an ADP System. In a remotely accessed resource-sharing system, the material can be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and access approvals. This mode of operation can accommodate the concurrent processing and storage of (a) two or more levels of classified data, or (b) one or more levels of classified data with unclassified data depending upon the constraints placed on the systems by the Designated Approving Authority (V. C.).

11. Operating System (O/S)

An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to a user and their programs and play a central role in assuring the secure operation of a computer system. Operating systems may perform debugging, input-output, accounting, resource allocation, compilation, storage assignment tasks, and other system related functions. (Synonymous with Monitor, Executive, Control Program, and Supervisor.)

12. Resource-Sharing Computer System

A computer system which uses its resources, including input/output (I/O) devices, storage, central processor (arithmetic and logic units), control units, and software processing capabilities, to enable one or more users to manipulate data and

5200.28(Encl 2)

Dec 18, 72

process co-resident programs in an apparently simultaneous manner. The term includes systems with one or more of the capabilities commonly referred to as time-sharing, multi-programming, multi-accessing, multi-processing, or concurrent processing.

13. Remotely Accessed Resource-Sharing Computer System

A computer system which includes one or more central processing units, peripheral devices, remote terminals, and communications equipment, or interconnection links, which allocates its resources to one or more user, and which can be entered from terminals located outside the central computer facility.

Additional definitions applicable to techniques and procedures for implementing, deactivating, testing, and evaluating secure resource-sharing ADP Systems are contained in DoD Manual 5200.28-M.

APPROVED 18 DEC 72



ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

COMPTROLLER

DoD 5200.28-M
ODASD(SP)

FOREWORD

This publication, DoD 5200.28-M, "Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating - Secure Resource-Sharing ADP Systems," is issued under the authority of and in accordance with DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems." This manual is effective immediately and is applicable to all Department of Defense Departments and Agencies, the Organization of the Joint Chiefs of Staff, and the Unified and Specified Commands which process, use, or store classified data, or generate classified information, in resource-sharing ADP systems. Its provisions are equally applicable to DoD operated systems, contractor operated systems, and to computer service organizations providing contractual ADP services to the Department of Defense or its contractors. This manual implements, DoD Directives and Instructions and takes precedence over conflicting instructions. It establishes uniform guidelines for techniques and procedures to be used when implementing, deactivating, testing, or evaluating secure resource-sharing ADP systems and, when applicable, components of such systems, without the necessity of further formal issuance by any DoD Component. The Heads of DoD Components may, however, augment this manual to meet their needs by prescribing more detailed guidelines and instructions for their systems which are not inconsistent with this manual and DoD Directive 5200.28. Two copies of each supplemental instruction issued by a Component shall be forwarded, immediately following publication, to the Deputy Assistant Secretary of Defense (Security Policy), OASD(C). One copy shall be appropriately marked to indicate the part of the manual which is being augmented. Recommendations for revisions or amendments to this publication should be addressed through appropriate channels to the Deputy Assistant Secretary of Defense (Security Policy), OASD(C).

R.E. McLoof

Assistant Secretary of Defense

CONTENTS

SECTION I

GENERAL PROVISIONS

Part 1. INTRODUCTION

<u>Paragraph</u>		<u>Page</u>
1-100	Objective - - - - -	1
1-101	Authority and Scope - - - - -	2
1-102	Responsibilities - - - - -	3
1-103	Arrangement - - - - -	5
1-104	Amendments - - - - -	5
1-105	Component Procedures - - - - -	6

Part 2. DEFINITIONS

1-200	Access - - - - -	7
1-201	Automatic Data Processing (ADP) System - - - -	7
1-202	ADP System Security - - - - -	8
1-203	Arrest - - - - -	8
1-204	Breach - - - - -	8
1-205	Briefing - - - - -	8
1-206	Central Computer Facility - - - - -	9
1-207	Compartmented Intelligence - - - - -	9

1-208	Contained - - - - -	9
1-209	Debriefing - - - - -	9
1-210	Dedicated Mode - - - - -	9
1-211	Escort(s)- - - - -	10
1-212	Evaluator(s) - - - - -	10
1-213	Evaluation - - - - -	10
1-214	Intelligence - - - - -	10
1-215	Investigation - - - - -	10
1-216	Material - - - - -	10
1-217	Multi-Level Security Mode - - - - -	11
1-218	Operating System (O/S) - - - - -	11
1-219	Orientation - - - - -	11
1-220	Penetration - - - - -	12
1-221	Resource-Sharing Computer System - - - - -	12
1-222	Remotely Accessed Resource-Sharing Computer System - - - - -	12
1-223	ST&E Tools and Equipment - - - - -	12
1-224	Validation - - - - -	12
1-225	Verification - - - - -	13

SECTION II

PERSONNEL SECURITY

Part 1. CLEARANCE AND ACCESS CONTROLS

2-100	General - - - - -	14
2-101	Central Computer Facility - - - - -	14
2-102	Operational and Operating System (O/S) Program- ming Personnel - - - - -	15
2-103	Hardward Maintenance Personnel - - - - -	15

SECTION III

PHYSICAL, COMMUNICATIONS, AND
EMANATIONS SECURITY

Part 1. PHYSICAL SECURITY OF AREAS

3-100	General - - - - -	16
3-101	Central Computer Facility - - - - -	16
3-102	Remote Terminal Areas - - - - -	16
3-103	Disconnect Procedures - - - - -	17
3-104	Supplemental Requirements - - - - -	17
3-105	Adjustment of Area Controls - - - - -	18

Part 2. PHYSICAL SECURITY OF EQUIPMENT

3-200	General - - - - -	19
3-201	Equipment Application - - - - -	19

Part 3. COMMUNICATIONS SECURITY

3-300	Communications Links - - - - -	20
3-301	Interface with Communications Networks - - - -	20
3-302	Storage and Forward Message Switches - - - - -	20
3-303	Multiplexers - - - - -	20

Part 4. EMANATIONS SECURITY

3-400	Emanations Control - - - - -	21
-------	------------------------------	----

SECTION IV

HARDWARE/SOFTWARE FEATURES

Part 1. GENERAL

4-100	Application - - - - -	22
-------	-----------------------	----

Part 2. HARDWARE

4-200	Hardware Features - - - - -	23
-------	-----------------------------	----

Part 3. OPERATING SYSTEM (O/S)

4-300	General - - - - -	25
4-301	O/S Controls - - - - -	25
4-302	Test and Debugging Programs - - - - -	26
4-303	Clear System Procedures - - - - -	26
4-304	Shutdown and Restart - - - - -	26
4-305	Other Fundamental Features - - - - -	26

SECTION V

AUDIT LOG OR FILE

Part 1. GENERAL

5-100	Application - - - - -	28
-------	-----------------------	----

SECTION VI

BASIC SAFEGUARDS

Part 1. GENERAL

6-100	Application - - - - -	29
-------	-----------------------	----

SECTION VII

ERASE AND DECLASSIFICATION PROCEDURES

Part 1. INTRODUCTION

7-100	General - - - - -	30
7-101	During Operations - - - - -	30

Part 2. ERASE PROCEDURES

7-200	General - - - - -	31
7-201	Magnetic Tapes - - - - -	31
7-202	Magnetic Discs, Disc Packs, Drums, and other Similar Rigid Magnetic Storage Devices - - - - -	31
7-203	Inoperative Magnetic Discs, Disc Packs, Drums, and Similar Rigid Storage Devices - - - - -	32

7-204	Internal Memory - - - - -	32
7-205	Magnetic Storage Media Used to Store Analog, Video, or Similar Non-Digital Information - - - -	32
Part 3. DISPOSITION APPROVAL		
7-300	General - - - - -	34
7-301	Records - - - - -	34
7-302	Specific Guidance - - - - -	34

SECTION VIII

SPECIFICATIONS FOR MAGNETIC TAPE ERASE EQUIPMENT

Part 1. EQUIPMENT SPECIFICATIONS

8-300	Magnetic Tape Degausser Specifications - - - - -	35
8-301	Requirements - - - - -	35
8-302	Test Procedure - - - - -	37

SECTION IX

SECURITY TESTING AND EVALUATIONS (ST&E)

Part 1. GENERAL

9-100	Purpose - - - - -	40
9-200	Procedures - - - - -	41

SECTION I

GENERAL PROVISIONS

Part 1. INTRODUCTION

1-100 Objective

The security of the United States depends in part upon the proper safeguarding of classified data processed, stored, and used in or classified information produced by ADP Systems. Safeguards applied to ADP Systems include all hardware/software functions, characteristics, and features; operational procedures, accountability procedures, and access controls at the central computer facility and remote computer and terminal facilities; and the management constraints and physical structures and devices needed to provide an acceptable level of protection for classified material (data or information) contained in the computer system.

a. The objective of this manual is to provide guidelines and establish techniques and procedures which can be used to:

1. Implement secure resource-sharing ADP Systems so that with reasonable dependability, deliberate or inadvertent access to classified material by unauthorized personnel or the unauthorized manipulation of the computer and its associated peripheral devices, which could lead to the compromise of classified information, can be prevented;
2. Develop, acquire, and establish methodologies, techniques, standards, and procedures for the design, analysis, testing, evaluation, and approval of the security features for resource-sharing ADP Systems;
3. Establish methodologies, techniques, and procedures for the physical protection of ADP Systems and components; and,
4. Prescribe standards, criteria, and specifications for deactivating secure ADP Systems and the sanitization of system components for disposition or utilization in unsecured environments.

b. The potential means by which a computer system can be adequately secured are virtually unlimited. The safeguards adopted must be consistent with available technology, the frequency of processing, the classification of the data handled or the information to be produced, the environment in which the ADP System operates, the degree of risk which can be tolerated, and other factors which may be unique to the installation involved. Rigid adherence to all techniques, methodologies, and requirements discussed in this manual could adversely impact upon the present and future use of the system under today's rapidly changing ADP technology. This technology is dynamic and the methods chosen to secure a particular system must accommodate new developments without degrading the level of protection.

* c. The techniques, methodologies, and procedures in this manual; however, represent an approved method of securing a remotely accessed resource-sharing computer system in a multi-level security mode as prescribed by DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems." It is understood that all of the techniques described in this manual may not be economically justified after a cost versus risk evaluation. Therefore, selected subsets of the techniques included in this manual, with appropriate trade-offs, may be used to gain the level of security required for classification category, etc., to be secured. In addition, techniques not necessarily included in this manual may be used so long as such methods provide the degree of security specified in DoD Directive 5200.28.

d. The techniques and procedures described in this manual shall not be applied to ADP Systems which cannot be retrofitted without excessive and unjustifiable costs or which can be dedicated and adequately secured for classified operations with reasonable administrative, personnel, physical and communication security controls.

1-101 Authority and Scope

a. This manual, authorized by the Secretary of Defense under the authority of the National Security Act of 1947, as amended, and E.O. 11652, is established as a DoD manual published by the Assistant Secretary of

Defense (Comptroller) under the authority of DoD Directive 5200.1, dated June 1, 1972, DoD Regulation 5200.1(R), June 1, 1972, DoD Directive 5100.40, dated May 18, 1970, as changed and DoD Directive 5200.28.

b. This manual is applicable to the Office of the Secretary of Defense, all Department of Defense Departments and Agencies, the Organization of the Joint Chiefs of Staff, and the Unified and Specified Commands, which process, use, or store classified data or produce classified information in resource-sharing ADP Systems. Its provisions are equally applicable to Department of Defense operated systems, contractor operated systems, and to computer service organizations providing contractual ADP services to the Department of Defense or its contractors wherein classified data and information are to be handled in a resource-sharing ADP System.

c. This manual implements DoD Directives and Instructions and the security policies established by the Assistant Secretary of Defense (Comptroller) and takes precedence over conflicting instructions. It establishes uniform guidelines for the techniques and procedures to be used when implementing, deactivating, testing, evaluating, and approving secure resource-sharing ADP Systems.

d. Recommendations for the clarification, revision, or amendment of this manual should be addressed with recommendations through channels to the Deputy Assistant Secretary of Defense (Security Policy), OASD(C).

1-102 Responsibilities

a. The Deputy Assistant Secretary of Defense (Security Policy), OASD(C), is designated to fulfill the responsibilities in Section V.A., DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," and to:

1. Approve all specialized security testing and evaluation (ST&E) tools and equipment validated for the joint usage of more than one Department of Defense Component or contractor;

2. Advise, assist, and assess progress of Department of Defense Components in the development and implementation of effective security testing and evaluation (ST&E) programs; and

3. Monitor administration of Component's ST&E programs.

b. Component's Designated Approving Authorities, or their designees for this purpose, in addition to the responsibilities assigned in Section V.C.1., 2., and 3., DoD Directive 5200.28, will assure:

1. Issuance of instructions which fully explain the security requirements and operating procedures of each ADP System approved for the handling of classified material and the proper clearance and indoctrination, in applicable security requirements and responsibilities, of all personnel who install, operate, maintain, or use such systems.

2. Operation of each ADP System under the controls prescribed for the category(ies) of classified material contained in the system.

3. Where appropriate, the appointment of terminal area security officer(s) who will be responsible for performing applicable security functions at approved terminal areas which are an integral part of an ADP System which contains classified material.

4. Maintenance of documentation on operating systems (O/S) and all modifications thereto, and its retention for a sufficient period of time to enable tracing of security-related defects to their point of origin or inclusion in the system.

5. Supervision, monitoring, and testing, as appropriate, of changes in an approved ADP System which could affect the security features of the system, so that a secure system is maintained.

6. Establishment of procedures to discover, recover, handle, and dispose of classified material improperly disclosed through system malfunction or personnel action.

7. Proper disposition and correction of security deficiencies in all approved ADP Systems, and the effective use and disposition of system housekeeping or audit records, records of security violations or security-related system malfunctions, and records of tests of the security features of the ADP System.

8. Conduct of competent system ST&E, timely review of system ST&E reports, and correction of deficiencies needed to support conditional or final approval or disapproval of the ADP System for the processing of classified information.

9. Establishment, where appropriate, of a central ST&E coordination point for the maintenance of records of selected techniques, procedures, standards, and tests used in the testing and evaluation of security features of ADP Systems which may be suitable for validation and use by other Department of Defense Components.

10. Justification of information requirements under the provisions of DoD Directive 5000.19.

11. Notification to the DASD(SP) of major ST&E plans, problems and accomplishments, as appropriate.

1-103 Arrangement

This manual is divided into sections, parts, and paragraphs. Each section is designated by subject and Roman numeral (e.g., I, II, III, etc.), and covers a separate aspect of implementing, deactivating, evaluating, testing, and approval of the security features of resource-sharing ADP Systems used to handle classified material. Each part is designated by title and Arabic numeral (e.g., 1., 2., 3., etc.), and contains a breakdown of the subjects covered by the section into related divisions. The paragraphs are a further division of the parts. They are so numbered that the first digit indicates the section, the second digit, the part and the last two digits, the paragraph (e.g., 1-103, designates Section I, part 1, paragraph 3; 2-314, designates Section II, part 3, paragraph 14). The manual is designed to permit subsequent insertions of additional looseleaf parts and paragraphs within the appropriate section without major reprint of the entire publication.

1-104 Amendments

This manual will be amended from time to time and, unless otherwise specified in any amendment, the amendment will be effective upon publication.

1-105 Component Procedures

Components may augment this manual to meet their needs by prescribing more detailed guidelines and instructions for their internal systems which are not inconsistent with this manual and DoD Directive 5200.28. The application of these provisions will be guided by the twofold objective of establishing reasonable uniformity and maintaining maximum cost effective security consistent with the accomplishment by each Component of its assigned mission. Two copies of each supplemental instruction issued by a Component shall be forwarded to the Deputy Assistant Secretary of Defense (Security Policy), OASD(C), immediately following publication. One copy shall be appropriately marked to indicate the part of this manual which is being augmented.

SECTION I

Part 2. DEFINITIONS

1-200 Access

The ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in an ADP System.

1-201 Automatic Data Processing (ADP) System

An assembly of computer equipment, facilities, personnel, software, and procedures configured for the purpose of classifying, sorting, calculating, computing, summarizing, storing, and retrieving data and information with a minimum of human intervention. ADP Systems as defined for purposes of this manual are the totality of Automatic Data Processing Equipment (ADPE) and include:

- a. General and Special purpose computers (e.g., digital, analog, or hybrid computer equipment);
- b. Commercially available components, those produced as a result of Research and Development, and the equivalent systems created from them, regardless of size, capacity, or price, which are utilized in the creation, collection, storage, processing, communication, display, and dissemination of classified information;
- c. Auxiliary or accessorial equipment, such as, data communications terminals, source data automation recording equipment (e.g., optical character recognition equipment, paper tape typewriters, magnetic tape cartridge typewriters, and other data acquisition devices), data output equipment (e.g., digital plotters and computer output microfilmers), etc., to be used in support of digital, analog, or hybrid computer equipment, either cable-connected, wire-connected, or self-standing;
- d. Electrical accounting machines (EAM) used in conjunction with or independently of digital, analog, or hybrid computers; and
- e. Computer equipment which supports or is integral to a weapons system.

1-202 ADP System Security

Includes all hardware/software functions, characteristics, and features, operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities, and; the management constraints, physical structures, and devices; personnel and communication controls needed to provide an acceptable level of protection for classified material to be contained (1-208) in the computer system.

1-203 Arrest

The discovery of user activity not necessary to the normal processing of data which might lead to a violation of system security and force termination of the activity.

1-204 Breach

The successful and repeatable defeat of security controls with or without an arrest (1-203), which if carried to consummation, could result in a penetration (1-220) of the system. Examples of breaches are:

- a. Operation of user code in master mode;
- b. Unauthorized acquisition of I.D. password or file access passwords; and
- c. Accession to a file without using prescribed operating system mechanisms.

1-205 Briefing

Explanation by a Test Team of the techniques, procedures, and requirements for the testing and evaluation of a specific system.

1-206 Central Computer Facility

One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area. This does not include remote computer facilities, peripheral devices, or terminals which are located outside the single controlled area even though they are connected to the central computer facility by approved communication links.

1-207 Compartmented Intelligence

Includes only that intelligence material having special controls indicating restrictive handling for which systems of compartmentation or handling are formally established.

1-208 Contained

"Contained" refers to a state of being within limits, as within system bounds, regardless of purpose or functions, and includes any state of storage, use, or processing.

1-209 Debriefing

The Test Team oral exit report of its evaluation of the security features of the ADP System.

1-210 Dedicated Mode

An ADP System is operating in a dedicated mode when the central computer facility and all of its connected peripheral devices and remote terminals are exclusively used and controlled by specified users or groups of users for the processing of a particular type(s) and category(ies) of classified material.

1-211 Escort(s)

Escort(s) are duly designated personnel who have appropriate clearances and access authorizations for the material contained in the system and are sufficiently knowledgeable to understand the security implications of and to control the activities and access of the individual being escorted. (Such action is essential to the protection of classified material contained in the system and to the maintenance of the reliability of the security features / hardware or software / of the system.)

1-212 Evaluator(s)

Personnel specifically designated to participate in the Test Team review, analysis, testing, and evaluation of the security features of an ADP System.

1-213 Evaluation

The evaluator's report to the Designated Approving Authority describing the investigative and test procedures used in the analysis of the ADP System Security features with a description and results of tests used to support or refute specific system weaknesses that would permit the acquisition of identifiable classified material from secure or protected data files.

1-214 Intelligence

Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all information concerning one or more aspects of foreign countries or areas, which is immediately or potentially significant to the development and execution of plans, policies, and operations.

1-215 Investigation

The review and analysis of system security features, (e.g., the investigation of system control programs using flow charts, assembly listings, and related documentation to determine the security provided by the operating system).

1-216 Material

"Material" refers to data processed, stored, or used in, and information produced by, an ADP System regardless of form or medium, e.g., programs, reports, data sets or files, records, and data elements.

1-217 Multi-Level Security Mode

A mode of operation under an operating system (supervisor or executive program) which provides a capability permitting various levels and categories or compartments of material to be concurrently stored and processed in an ADP System. In a remotely accessed resource-sharing system, the material can be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and access approvals. This mode of operation can accommodate the concurrent processing and storage of (a) two or more levels of classified data, or (b) one or more levels of classified data with unclassified data depending upon the constraints placed on the systems by the Designated Approving Authority (V.C.).

1-218 Operating System (O/S)

An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in assuring the secure operation of a computer system. Operating systems may perform debugging, input-output, accounting, resource allocation, compilation, storage assignment tasks, and other system related functions (Synonymous with Monitor, Executive, Control Program, and Supervisor.)

1-219 Orientation

The formal and informal presentations and discussions with the authority responsible for the ADP System which supplements the information in the initial Security Testing and Evaluation (ST&E) Request and provides the system evaluators an introduction to the operating environment, the techniques used to provide system security, the identity and location of documentation describing the implementation of system security measures (e.g., O/S modifications, etc.), and the techniques available to demonstrate the effectiveness of such measures in meeting requirements of DoD Directive 5200.28.

1-220 Penetration

The successful and repeatable extraction and identification of recognizable information from a protected data file or data set without any attendant arrests.

1-221 Resource-Sharing Computer System

A computer system which uses its resources, including input/output (I/O) devices, storage, central processor (arithmetic and logic units), control units, and software processing capabilities, to enable one or more users to manipulate data and process co-resident programs in an apparently simultaneous manner. The term includes systems with one or more of the capabilities commonly referred to as time-sharing, multi-programming, multi-accessing, multi-processing, or concurrent processing.

1-222 Remotely Accessed Resource-Sharing Computer System

A computer system which includes one or more central processing units, peripheral devices, remote terminals, and communications equipment or interconnection links, which allocates its resources to one or more user, and which can be entered from terminals located outside the central computer facility.

1-223 ST&E Tools and Equipment

Specialized techniques, procedures, criteria, standards, programs, or equipment accepted by qualified Security Testing and Evaluating (ST&E) personnel for uniform or standard use in testing and evaluating secure features of ADP Systems.

1-224 Validation

That portion of the development of specialized ST&E procedures, tools, and equipment needed to establish acceptance for joint-usage by one or more DoD Components or their contractors. Such action will include, as necessary, final development, evaluation, and testing leading to acceptance, by senior ST&E staff specialists of the three Military Departments or a Defense Agency, and approval for joint usage by the DASD(SP).

1-225 Verification

The successful testing and documentation of actual on-line system penetration or attempts to penetrate the system in support or in contradiction of assumptions developed during system review and analysis which are to be included in the Evaluation report.

SECTION II

PERSONNEL SECURITY

Part 1. CLEARANCE AND ACCESS CONTROLS

2-100 General

Personnel who develop, test(debug), maintain, or use programs which are classified or which will be used to access or develop classified material shall have a personnel security clearance and an access authorization(need-to-know), as appropriate for the highest classified and most restrictive category of classified material which they will access under system constraints.

2-101 Central Computer Facility

- a. Unescorted entry to the Central Computer Facility or access to any of its ADP System components (hardware or software) shall be controlled and limited to personnel who are cleared for access to the highest classified and most restricted category of classified material contained in the ADP System, and whose need-to-know has been ascertained by the responsible ADP Systems Security Officer.
- b. When the ADP System contains compartmented intelligence or SIOP-ESI, access shall be limited to personnel who, in addition to the above, have a TOP SECRET clearance and an access authorization, as appropriate, for the type(s) of material contained in the system. Except as specified in Subsection 2-103, below, other persons, whose access to the area is required on a one-time or infrequent basis and who will not have access to classified material or to the system's hardware or software, may be admitted to the area when accompanied by an escort, (paragraph 1-211) who will be responsible for the visitor's activities while in the area.

2-102 Operation and Operating System (O/S) Programming Personnel

Personnel operating the system and controlling access to its entry points or those who design, develop, install, modify, service, or maintain the security features of the software in the operating system (O/S) which controls user program access to the system (I/O, storage or use) or the key or combination by which the system is protected, shall be cleared and have access authorization as appropriate for the highest classified and most restrictive category of material contained in the system and shall be indoctrinated in appropriate security procedures for the particular ADP System and facility before assuming their duties. (Temporary or permanent modification of the O/S shall be tested by designated personnel to assure that the security features of the ADP System are effective. Audit trail records [Subsection 5-100] of these transactions shall be maintained.)

2-103 Maintenance Personnel

Personnel requiring access to any part or component of the ADP System (central or remote) which could affect or modify the secure operations of the system or permit access to classified data or information, shall have a security clearance and access authorization for the highest classified and most restrictive category of classified material contained in the system. Should it become necessary for uncleared maintenance personnel to access the ADP System they shall be accompanied by an escort (See 1-211) designated for that purpose.

SECTION III

PHYSICAL, COMMUNICATIONS, AND EMANATIONS SECURITY

Part 1. PHYSICAL SECURITY OF AREAS

3-100 General

Physical security considerations are essential elements in the planning, design, installation, utilization, and evaluation of all ADP System facilities and installations.

3-101 Central Computer Facility

a. Physical security requirements for the central computer facility area will be commensurate with the highest classified and most restrictive category of information being handled in the ADP System.

b. If two or more computer systems are located in the same controlled area, the equipment comprising each system may be located so that direct personnel access, if appropriate, will be limited to a specific system.

3-102 Remote Terminal Areas

a. While the physical and personnel security requirements for the Central Computer Facility area are based upon the overall requirements of the total ADP System, remote terminal area requirements will be based upon the highest classified and most restrictive category and type of material which will be accessed through the terminal under system constraints.

b. Each remote terminal will be individually identified to ensure required security control and protection, with identification as a feature of hardware in combination with the operating system.

c. When a peripheral device or remote terminal, whether or not approved for the handling of classified material, is to be used by personnel of a component that is not responsible for the over-all operation and control of the ADP System, the security measures for the device or terminal and its area will be prescribed by the authority responsible for the security of the over-all ADP System. Such security measures will be agreed to and implemented before the user's peripheral device or remote terminal may be connected to the ADP System.

d. When one or more DoD Components' ADP Systems become a part of a larger ADP network, the approval and the authority to authorize temporary exceptions to security measures for the Components' ADP System in the network will require the concurrence and approval of both the DoD component operating the ADP System and the DoD component having over-all responsibility for the security of the network. (See para. 3-301.)

3-103 Disconnect Procedures

a. Each remote terminal which is not controlled and protected, as required for material accessible through it will be disconnected from the ADP System when the system contains classified information.

b. Disconnect procedures, when required to protect classified material contained in the ADP System, will be used to disconnect remote I/O terminals and peripheral devices from the system by a hardware or software method authorized by the Designated Approving Authority.

3-104 Supplemental Requirements

When compartmented intelligence or SIOP-ESI is to be handled in the ADP System, the supplemental physical security control required by Sections IV, L, and M of DoD Directive 5200.28, will apply to the central computer facility area, and all areas having remote terminals connected to the system.

3-105 Adjustment of Area Controls

a. When appropriate, provision will be made to permit adjustment of area controls to the level of protection required for the category or type of material actually being handled in the computer, its peripheral devices, and terminals, except that the Central Computer Facility and those components approved for the storage and processing of classified material, will not be downgraded below the level required to protect secure communications equipment, to maintain the reliability and security of the ADP System, and to protect essential hardware or software components of the ADP System.

b. If the minimum measures for the Central Computer Facility, or ADP System are suspended or discontinued for any reason, the security features of the system will be re-evaluated, as would any new system or component before again being approved for the processing of classified material.

SECTION III

Part 2. PHYSICAL SECURITY OF EQUIPMENT

3-200 General

While procedural or specialized techniques to be applied by Components, have, in the past, been largely left to their discretion, it is contemplated that as specialized techniques are developed and tested they will be published either in this manual or its associated newsletter.

3-201 Equipment Application

Counter-measures to Physical Security Hazards such as fire, natural disaster, sabotage, and environmental problems (e.g., power failures) are also being prepared for coordination, approval, and publication in this section of the manual.

SECTION III

Part 3. COMMUNICATIONS SECURITY

3-300 Communication Links

Transmission and communication lines and links which provide secure communications between components of or to an ADP System will be secured in a manner appropriate for the material designated for transmission through such lines or links under the provisions of DoD Directive C-5200.5, DoD Directive 5200.1, and DoD Regulation 5200.1(R). Telecommunications facilities supporting ADP Systems will meet the security criteria used for Defense Communications System under DoD Directive 4630.1.

3-301 Interface with Communications Networks

The DoD component that operates an ADP System which requires only communication support from telecommunications networks such as AUTODIN will determine the security requirements for the handling of classified material in its ADP System. The security measures to be agreed to and implemented before connection with the communication network are limited to those needed to insure the development, interface, and integration of secure, reliable, survivable, and cost-effective transmission and communication lines and links which are needed to meet the communication requirements of the telecommunications network supporting the ADP System.

3-302 Storage and Forward Message Switches

Information in this section will be added following further coordination and approval.

3-303 Multiplexers

Information in this section will be added following further coordination and approval.

SECTION III

Part 4. EMANATIONS SECURITY

3-400 Emanations Control

Measures to control compromising emanations are subject to approval under the provisions of DoD Directive S-5200.19, by the cognizant authority of the Component approving the security features of the ADP System. Application of these measures within industrial ADP Systems is only at the direction of the contracting activity concerned under provisions of Section IV.N. of DoD Directive 5200.28, and the requirements are to be included in the contract.

SECTION IV

HARDWARE/SOFTWARE FEATURES

Part 1. GENERAL

4-100 Application

A combination of hardware and software features are essential to provide protection for material stored or processed in the secure resource-sharing ADP System. While all of the following features may not be available in the current hardware or software or a combination thereof, they shall be provided at the earliest date that the state-of-the-art permits. The available hardware/software features outlined below should operate unabridged whenever classified material is contained in the resource-sharing ADP System and measures shall be implemented to provide special controls over the access to or modification of such features. Where possible and practicable, such features should contain two or more independent controls which would have to malfunction simultaneously for a breach of system security to occur.

SECTION IV

Part 2. HARDWARE

4-200 Hardware Features

- a. The execution state of a processor should include one or more variables, i. e., "protection state variables", which determine the interpretation of instructions executed by the processor. For example, a processor might have a master mode/user mode protection state variable, in which certain instructions are illegal except in master mode. Modification of the protection state variables shall be so constrained by the operating system and hardware that a user cannot access information for which he has no authorization.
- b. The ability of a processor to access locations in memory (hereinafter to include primary and auxiliary memory) should be controlled (e. g., in user mode, a memory access control register might allow access only to memory locations allocated to the user by the O/S).
- c. The operation of certain instructions should depend on the protection state of the processor. For example, instructions which perform input or output operations would execute only when in master mode. Any attempt to execute an instruction which is not authorized should result in a hardware interrupt which will permit the O/S to interrupt and/or abort the program containing the illegal instruction.
- d. All possible operation codes, with all possible tags or modifiers, whether legal or not, should produce known responses by the computer.
- e. All registers should be capable of protecting their contents by error detection or redundancy checks. These include those which set protection state variables, control input or output operations, execute instructions, or which are otherwise fundamental to the secure operation of the hardware.

f. Any register which can be loaded by the operating system should also be storable, so as to permit the O/S to check its current contents against its presumed contents. (The term "register" as used in e. and f. refers primarily to index or general purpose registers rather than an isolated address of a single storage location within the computer.)

g. Error detection should be performed on each fetch cycle of an instruction and its operand (e.g., parity check and address bounds check).

h. Error detection (e.g., parity checks) and memory bounds checking should be performed on transfers of data between memory and storage devices or terminals.

i. Automatic programmed interrupt should function to control system and operator malfunction.

j. The identity of remote terminals for input or output should be a feature of hardware in combination with the operating system.

k. Read, write, and execute access rights of the user should be verified on each fetch cycle of an instruction and its operand.

SECTION IV

Part 3. OPERATING SYSTEM (O/S)

4-300 General

The user and master modes of ADP Systems operation shall be separated so that a program operating in a user mode is prevented from performing control functions. As much of the operating system (O/S) as possible should run in the user mode (as opposed to the master mode) and each part of the O/S should have only as much freedom of the computer as it needs to do its job.

4-301 O/S Controls

The O/S shall contain controls which provide the user with all material to which he is authorized access, but no more. If such controls are not feasible, output material shall be generated only within the central computer facility under the cognizance of the ADP System Security Officer. As a minimum, the O/S must control:

- a. All transfers of material between memory and on-line storage devices; between the central computer facility equipment and any remote device; or between on-line storage devices; and
- b. All operations associated with allocating ADP System resources, (e.g., memory, peripheral devices, etc.) memory protection, system interrupt, and shifting between user and master protection modes; and
- c. Access to programs and utilities which are authorized to perform the various categories of maintenance (e.g., as operations which effect authorized additions, deletions, or changes to data) on the operating system, including any of its elements and files. Such controls shall insure that access is limited to personnel authorized to perform particular categories of maintenance; and
- d. All other programs (user programs) so that access to material is made via an access control and identification system which associates the user and his terminal, in the ADP System, with the material being accessed.

4-302 Test and Debugging Programs

User application programs, and systems programs which do not violate the security or integrity of the ADP System, may be debugged during system operation, provided that such activity is limited to the user mode. All other system software development, experimentation, testing, and debugging shall be performed on a system temporarily dedicated for these purposes.

4-303 Clear System Procedures

Procedures shall be available for clearing from the system, or making inaccessible, all classified material during operations without the required protection.

4-304 Shutdown and Restart

The O/S must provide for security safeguards to cover unscheduled system shutdown (aborts) and subsequent restart, as well as for scheduled system shutdown and operational start-up.

4-305 Other Fundamental Features

The following features of the operating system (O/S) are also considered fundamental to the secure operation of an ADP System. Unauthorized attempts to change, circumvent, or otherwise violate these features should be detectable and reported within a known time by the operating system causing an abort or suspension of the responsible user activity. In addition, the incident shall be recorded in the audit log, and the ADP System Security Officer notified.

a. Memory/Storage Protection - The Operating System shall protect the security of the ADP System by controlling:

1. Resource allocation (including primary and auxiliary memory);
2. Memory access outside of assigned areas; and
3. The execution of master (supervisory) mode instructions which could adversely affect the security of the O/S.

b. Memory Residue:- The O/S shall ensure that classified material or critical elements of the system do not remain as accessible residue in memory or on on-line storage devices.

c. Access Controls:- Access to material stored within the ADP System shall be controlled by the ADP System Security Officer, as required by cognizant authority, or by automatic processes operating under separate and specific controls within the O/S established through hardware, software, and procedural safeguards approved by the ADP System Security Officer.

d. Security Labels - All classified material accessible by or within the ADP System shall be identified as to its security classification and access or dissemination limitations, and all output of the ADP System shall be appropriately marked.

e. Terminal Identification:- Manual and administrative procedures and/or appropriate hardware/software measures shall be established to assure that the terminal from which personnel are attempting to access classified material has been protected and is authorized such access. Where a terminal identifier is used, for this purpose, it shall be maintained in a protected file.

f. User Identification:- Where needed to assure control of access and individual accountability, each user or specific group of users shall be identified to the ADP System by appropriate administrative or hardware/software measures. Such identification measures must be in sufficient detail to enable the ADP System to provide the user only that material which he is authorized.

SECTION V

AUDIT LOG OR FILE

Part 1. GENERAL

5-100 Application

An audit log or file (manual, machine, or a combination of both) shall be maintained as a history of the use of the ADP System to permit a regular security review of system activity. (e.g. The log should record security related transactions, including each access to a classified file and the nature of the access, e.g. logins, production of accountable classified outputs, and creation of new classified files. Each classified file successfully accessed /regardless of the number of individual references/ during each "job" or "interactive session" should also be recorded in the audit log. Much of the material in this log may also be required to assure that the system preserves information entrusted to it.)

SECTION VI

BASIC SAFEGUARDS

Part 1. GENERAL

6-100 Application

Procedures and basic safeguards prescribed in DoD Directive 5200.1, and DoD Regulation 5200.1(R), for the transmission, processing, handling, storage, and disposal of classified material apply to the material removed from the custody of the system. Further, when located outside of the central computer facility or its approved remote terminal areas all disc packs, tapes, etc., used to store classified material shall be protected and stored as appropriate for the classification of the highest category of material ever recorded thereon until declassified (see Section VII).

SECTION VII

ERASE AND DECLASSIFICATION PROCEDURES

Part 1. INTRODUCTION

7-100 General

The following procedures and specifications result from extensive research, investigation, and practice. They are adequate to the extent of such research and investigation, but, do not necessarily represent the ultimate status to be reached in this aspect of computer security. It is, therefore, anticipated that they will be improved through continued testing, evaluation, and usage by DoD Components.

7-101 During Operations - During normal operations in a controlled environment each memory location used for the storage of classified data shall be overwritten when it is no longer required, before re-utilization, or before the content of the location may be read to preclude the unauthorized disclosure of classified data. Hardware/ software techniques may be used to accomplish this task. When any of the memory units or storage media are removed from the controlled environment, the procedures in Section VII Part 2., below, shall apply.

SECTION VII

Part 2. ERASE PROCEDURES

7-200 General

a. Safeguarding classified information in a computer or computer system requires special precautions because of the type of storage media and devices (magnetic drums, discs, disc packs, and tapes) used to store, record, or manipulate data which must be protected by appropriate classification and security controls until procedures below are carried out.

b. Declassification - The eventual temporary or outright release of the storage device or a system including storage media should be anticipated. Procedures to be used to release or deploy the storage media are as follows:

7-201 Magnetic Tapes

Tapes used to store magnetically recorded digital data may be declassified by erasing with bulk tape degaussers which have been tested and approved by a laboratory of a Department of Defense Component or a commercial testing laboratory, where such tests may be certified, by adhering to test methods and performance criteria in technical specifications promulgated in Section VIII. Elements of DoD Components may, where necessary, develop procurement specifications for their use, provided the test methods and performance criteria comply, as a minimum, with the specifications in Section VIII.

7-202 Magnetic Discs, Disc Packs, Drums, and other Similar Rigid Magnetic Storage Devices

The equipment shall be checked immediately prior to beginning the overwrite procedure to insure that malfunctions do not occur which will prevent the classified information from being effectively overwritten. Further, when the capability exists, as an integral part of

the storage subsystem, an AC/DC erase will be applied to all data tracks before the tracks are overwritten and the overwrite verified. Thereafter, all storage locations will be overwritten a minimum of three times, once with the binary digit "1", once with the binary digit "0", and once with a single numeric, alphabetic, or special character. Such alpha-numeric or other unclassified data shall be left on the device. The current used in overwriting must be equal to that used in recording the information, but of a strength which will not damage or impair the equipment.

7-203 Inoperative Magnetic Discs, Disc Packs, Drums, and Similar Rigid Storage Devices

If the storage device has failed in such a manner that it cannot be overwritten, the device may be declassified by exposing the recording surface(s) to a permanent magnet having a field strength at the recording surface of at least 1,500 OERSTED. Care must be taken to insure that entire surface is wiped at least three times, by a non-uniform motion of the magnet. Care must be taken to assure that all tracks are covered by the center of the magnet. A thin sheet of clear plastic (a 1-5 mil sheet) should be used to prevent damage to the recording surface(s).

7-204 Internal Memory

Internal memory (e.g., core) may be declassified by alternately setting each addressable memory location alternately to all "ones" and all "zeros" for 1000 cycles until the state is changed at least 999 times. Detailed memory erase or clearing programs or routines should be prepared by qualified ADP programmers and approved by the ADP Systems Security Officer.

7-205 Magnetic Storage Media Used to Store Analog, Video, or Similar Non-Digital Information

Magnetic tape used to record analog, video, or similar types of non-digital information may be declassified by degaussing as in 7-201.

above. Rigid magnetic storage surfaces may be declassified as in 7-202, above, except that the unclassified overwriting signal must be analog instead of binary with the latter recording left intact on the device. In the case of a failure of the degausser or overwriting methods, a permanent magnet may be used as in 7-203, above, for rigid recording surfaces.

SECTION VII

Part 3. DISPOSITION APPROVAL

7-300 General

With the specific approval in each case of the Designated (systems) Approving Authority, or his designee for this purpose, within the DoD Component that is responsible for the security features of the ADP System, storage media treated as above may be handled as unclassified and released as necessary.

7-301 Records

A record of the above operations shall be maintained for a period of two (2) years after disposition of the device or equipment.

7-302 Specific Guidance

- a. Guidance for eradication of magnetic media not covered above may be obtained by submission of all pertinent details to the Deputy Assistant Secretary of Defense (Security Policy), OASD(C), for consideration on a case-by-case basis.
- b. In the absence of eradication by approved equipment or procedures, or at the direction of the designated official responsible for the ADP System's security features, magnetic information storage media shall be safeguarded in the manner prescribed for the highest classification ever recorded thereon until it is destroyed.

SECTION VIII

SPECIFICATIONS FOR MAGNETIC TAPE ERASE EQUIPMENT

Part 1. EQUIPMENT SPECIFICATIONS

8-300 Magnetic Tape Degausser Specifications

This specification covers an equipment to be used for automatic bulk degaussing of recorded magnetic tape. It describes in general the desired configuration and sets forth desired electrical and magnetic performance.

8-301 Requirements

a. General

1. Reel Size. The equipment shall be designed to degauss magnetic tape in widths from 1 to 2 inches, wound on reels from 3 to 15 inches in diameter, with provision for conversion to either 5/16 inch hubs or computer reel hub dimensions. It will be permissible to turn over 2 inch reels for degaussing.

2. Installation. The equipment shall be designed such that either rackmounting or bench top operation can be accommodated with minimum modification.

3. Operation. Operation shall be automatic once the reel is loaded and the degaussing cycle is initiated, except for 2 inch wide tape which may be cycled twice. The degaussing operation shall not require more than two minutes per reel.

4. Degaussing Safeguard. A method of monitoring the relative current in the degaussing coils shall be provided.

5. Safeguard Tape Unwinding. For vertically mounted degaussers, a method of reversing the direction of reel rotation while cycling shall be provided. This reversal of reel direction must not interrupt the degaussing cycle. This safeguard prevents the unwinding of tape while cycling.

b. Detailed Requirements

1. Electrical Power. The equipment must meet all requirements over the following parameter ranges:

- (a) Input Voltage Range - 95 to 135 VAC, single phase, three wire system.
- (b) Line Frequency Range - 48 to 62 cycles per second.
- (c) Power - The current drain shall be less than 20 amperes for any of the foregoing conditions of line frequency and voltage.

c. Mechanical

1. Cabinet. The equipment shall be designed for mounting in a standard 19 inch rack and shall have minimum height and weight according to the design requirements.

2. Finish. Surfaces shall be adequately protected against corrosion within the environments detailed under section d., below.

d. Environmental Performance. The equipment shall perform to specification when operated in the environments listed in the following paragraphs:

- 1. Altitude. Non-operating: sea level to 50,000 feet
Operating: sea level to 10,000 feet
- 2. Relative Humidity. Operating and non-operating; 5 to 100 percent, no condensation. However the equipment shall survive condensation after being dried out.
- 3. Temperature. Non-operating: -40° to 71° C
Operating: 0° C to $+55^{\circ}$ C
- 4. Vibration and Shock. Non-operating. The equipment shall survive specified test methods which are intended to simulate shock and vibration levels expected in commercial shipping and handling.

e. Performance.

1. Degaussing Level. The residual signal level after degaussing shall be a minimum of 90 db below saturated signal level for tape widths of 1 inch or less.

2. Duty Cycle. Design shall be such that continuous operation, i.e., a duty cycle of 100% may be used. Under conditions of continuous operation, the temperature rise at the reel face of the equipment shall not exceed 35°F above ambient.

8-302 Test Procedure.

a. Equipment.

1. Recorder/Reproducer with full track 1/4" heads.
2. Audio Oscillator
3. Wave Analyser with 20 ops bandwidth
4. Oscilloscope

b. Procedure.

1. Record. Record tapes with a 400 ops signal at 7' ips with the record level set for saturation. Measure the playback signal level using the wave analyser on the 20 ops bandwidth position and the recorder playback gain set at maximum. This is the reproduce reference level.

NOTE: The saturation point shall be defined by the tape transfer curve as the output level for which input levels 1 and 2 produce the same output. (See Figure No. 1)

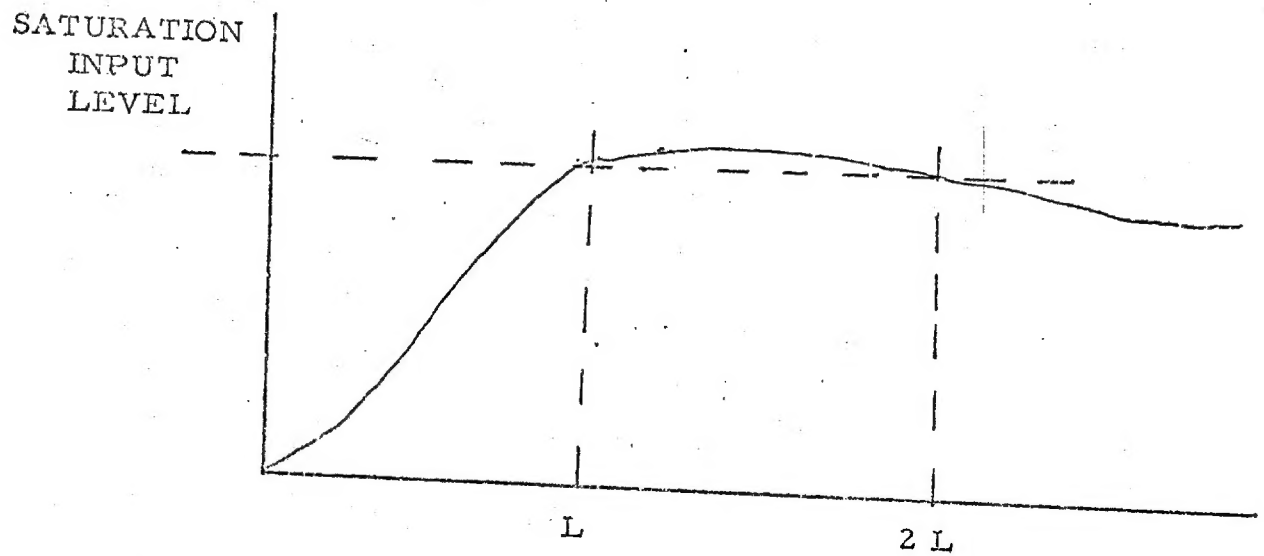
2. Degaussing. Degauss the tapes.

NOTE: To evaluate the ability to degauss wider tape widths two, three, and four 1/4 inch reels can

be taped together for the degaussing procedure. To simulate the larger diameter reels a special 15" X 1/4" reel would have to be used. This can be constructed by interchanging a standard 1/4" hub and 15" flanges.

3. Playback. Playback the degaussed tapes with the playback gain set at maximum. Tune the wave analyzer (20 ops bandwidth) to measure any residual signal level,

NOTE: Clean and degauss tape recorder threading path before each pass.



SECTION IX

SECURITY TESTING AND EVALUATIONS (ST&E)

Part 1. GENERAL

9-100 Purpose

- a. To develop and acquire methodologies, techniques, and standards for the analysis, testing, and evaluation of the security features of ADP Systems.
- b. To assist in the analysis, testing, and evaluation of the security features of ADP Systems by developing facts (for the Designated Approving Authority) concerning the effectiveness of measures used to secure the ADP System in accordance with Section VI of DoD Directive 5200.28, and the provisions of this Manual. (See Sections II, III, and IV.)
- c. To minimize duplication and overlapping of effort, improve the effectiveness and economy of security operations, and provide for the approval and joint usage of ST&E Tools and Equipment.

SECTION IX

Part 2.

9-200 Procedures

The procedures and other portions of this section will be published following additional testing and coordination.